ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●偽のセキュリティ警告・サポート詐欺によるPCへの侵入か…約15,000人の個人情報流出の可能性

https://www.itmedia.co.jp/news/articles/2403/21/news164.html
https://www.city.yaizu.lg.jp/business/suisan-nougyo/fisheries/shinsosui/info.html

このニュースをザックリ言うと･･･

- 3月18日(日本時間)、静岡県焼津市より、同市施設「焼津市駿河湾深層水脱塩施設」利用者の個人情報が流出した可能性があると発表されました。

- 被害を受けたのは、同施設の利用登録者約15,000人分の氏名・住所・電話番号および登録番号・登録日とされており、クレジットカード番号・金融機関口座番号などの情報は含まれてないとのことです。

- 情報を管理していた、施設の運営委託先のPCにおいて、同14日に「ウイルスに感染した」といった警告が表示、職員が表示された電話番号に電話をかけて「対応」を受けており、翌日別の職員が当該PCの電源を入れたところ見慣れない画面が表示されたことから、情報が流出した恐れがあると判断しています。

AUS便りからの所感等

- PCが実際にマルウェアに感染していたか否かの断定はできませんが、偽のセキュリティ警告により、サポートを騙る攻撃者がPCに遠隔操作で侵入した可能性が高く、これによってPC上の個人情報を持ち出された(また報道によれば金銭被害も受けた)とみられます。

- マルウェアに感染していなかったとしても、通常のWebサイトに表示される広告からの誘導先で偽のセキュリティ警告が表示される事例、またブラウザーのデスクトップ通知を悪用し、安易に通知を許可したユーザーに対し偽の警告を表示する事例も報告されています。

- IPAでは、偽のセキュリティ警告がどう表示されるかを体験できるサイトを昨年12月に公開しており(AUS便り 2023/12/20号参照)、このような攻撃者の手口があることを事前に把握し、慎重に行動することが重要です。

ITmedia NEWS

焼津市、深層水の購入者1万5000人の個人情報漏えいか　原因は「サポート詐欺」

2024年03月21日 16時38分 公開　[芹澤隆徳，ITmedia]

静岡県焼津市は、市内にある「焼津市駿河湾深層水脱塩施設」を利用した約1万5000人の個人情報が漏えいしたおそれがあると発表した。業務委託先の従業員が「サポート詐欺」にかかったとみられる。

「焼津市駿河湾深層水脱塩施設」（市のWebサイトより）

漏えいのおそれがある個人情報は、施設を利用する際に登録した氏名、住所、電話番号、そして登録日と登録番号。クレジットカード番号などの情報は含まれてない。

●個人情報191人分入ったUSBメモリー紛失…暗号化パスワード、本体に貼り付け

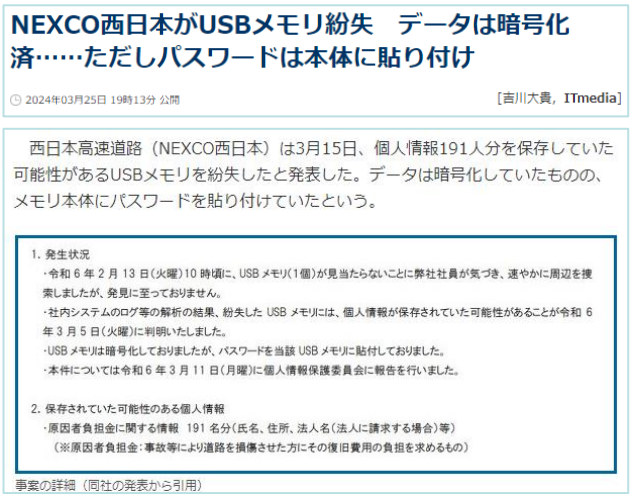
https://www.itmedia.co.jp/news/articles/2403/25/news170.html
https://www.w-nexco.co.jp/emc/emcpdfs/20240315135608-01.pdf

このニュースをザックリ言うと･･･

- 3月15日(日本時間)、NEXCO西日本より、個人情報が保存されていたUSBメモリーを紛失していたと発表されました。
- 保存されていたのは、原因者負担金(事故により道路損傷させた者に復旧費用の負担を求める)に関する191人分の氏名・住所および法人名等とされています。
- 2月13日にUSBメモリーの所在が分からないことに気付き、以後も発見に至っていないとのことです。
- またUSBメモリーのデータは暗号化されていますが、暗号化のパスワードを本体に貼り付けていたとしています。

AUS便りからの所感

- 紛失の可能性、紛失時の情報流出のリスクが高いにも拘らず、依然「USBメモリーにデータを保存して持ち運ぶ」運用が行われ、例えば委託先にもそれが要求され、実際に紛失する事例は後を絶ちません。
- 今回については、近年問題にされた「暗号化ZIPファイルとそのパスワードをメールで送る」ことと、「なぜ暗号化の意味がなくなるのか」という点では似通っており、端的に言えば、暗号化でデータを保護するという目的を果たすには、パスワードを暗号化されたデータと完全にセットとせず、別の手順・経路で渡し、保管することが重要です。



ITmedia NEWS

NEXCO西日本がUSBメモリ紛失　データは暗号化済……ただしパスワードは本体に貼り付け

2024年03月25日 19時13分 公開　[吉川大貴，ITmedia]

西日本高速道路（NEXCO西日本）は3月15日、個人情報191人分を保存していた可能性があるUSBメモリを紛失したと発表した。データは暗号化していたものの、メモリ本体にパスワードを貼り付けていたという。

1. 発生状況
・令和 6 年 2 月 13 日（火曜）10 時頃に、USB メモリ（1 個）が見当たらないことに弊社社員が気づき、速やかに周辺を捜索しましたが、発見に至っておりません。
・社内システムのログ等の解析の結果、紛失した USB メモリには、個人情報が保存されていた可能性があることが令和 6 年 3 月 5 日（火曜）に判明いたしました。
・USB メモリは暗号化しておりましたが、パスワードを当該 USB メモリに貼付しておりました。
・本件については令和 6 年 3 月 11 日（月曜）に個人情報保護委員会に報告を行いました。

2. 保存されていた可能性のある個人情報
・原因者負担金に関する情報　191 名分（氏名、住所、法人名（法人に請求する場合）等）
（※原因者負担金：事故等により道路を損傷させた方にその復旧費用の負担を求めるもの）

事案の詳細（同社の発表から引用）

●20年以上更新のない解凍ツールに脆弱性、開発者連絡取れず…利用中止呼び掛け

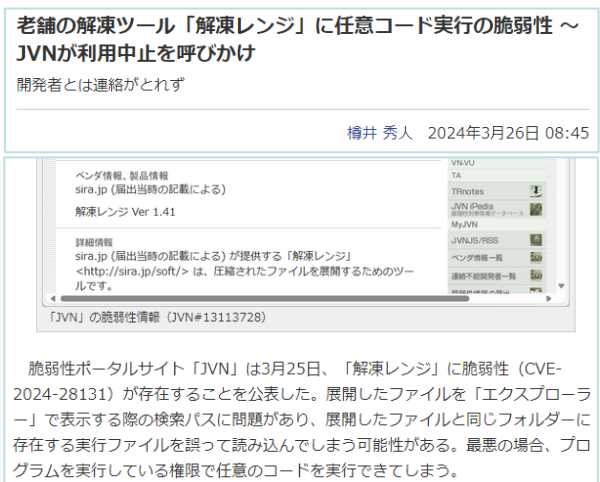
https://forest.watch.impress.co.jp/docs/news/1578919.html
https://jvn.jp/jp/JVN13113728/

このニュースをザックリ言うと･･･

- 3月25日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、圧縮ファイル解凍用Windowsツール「解凍レンジ」に脆弱性が存在するとして注意喚起が出されています。
- 注意喚起によれば、「展開したファイルをエクスプローラーで表示する際の実行ファイル検索パスに問題があり、展開したファイルと同じフォルダに存在している実行ファイルを読み込んでしまう脆弱性」があるとしています。
- 2002年6月に公開された最新バージョン1.41までに脆弱性が確認されており、また開発者と連絡が取れず対策状況が不明であることから、JVNでは当該ソフトの使用中止を呼び掛けています。

AUS便りからの所感

- 3月27日現在、Chrome・Edge・Firefoxといった主なWebブラウザーにおいて、解凍レンジのインストーラーを公式サイトからダウンロードしようとした場合に警告が表示されるようになっています。
- 類似した脆弱性として、実行するプログラムと同じフォルダーにあるDLLファイルを読み込むというものがあり、2017年以降「DLLインジェクション攻撃」を引き起こす問題が指摘され、多くのソフトウェアで修正されています。
- 例えば90年代末～2000年代に人気を博したソフトウェアが更新停止後も使い続けられるケースは珍しくありませんが、今回のように脆弱性が報告されたものでなくとも、未公開の脆弱性が密かに攻撃者に悪用される恐れは十分にあり、その場合に対策されることが期待できないことを鑑み、使用しているソフトウェアがメンテナンスされているか確認し、さもなくば他のソフトに乗り換えることを検討すべきです。



Impress Watch

老舗の解凍ツール「解凍レンジ」に任意コード実行の脆弱性 ～JVNが利用中止を呼びかけ

開発者とは連絡がとれず

樽井 秀人　2024年3月26日 08:45

「JVN」の脆弱性情報（JVN#13113728）

脆弱性ポータルサイト「JVN」は3月25日、「解凍レンジ」に脆弱性（CVE-2024-28131）が存在することを公表した。展開したファイルを「エクスプローラー」で表示する際の検索パスに問題があり、展開したファイルと同じフォルダーに存在する実行ファイルを誤って読み込んでしまう可能性がある。最悪の場合、プログラムを実行している権限で任意のコードを実行できてしまう。